EXPERTCHOICE
first to reach the goal

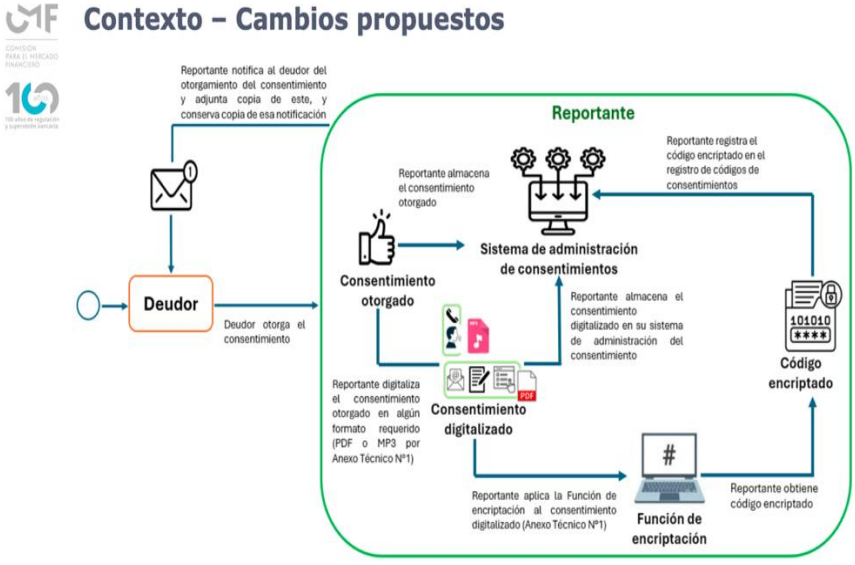
Gestor de Consentimientos
REDEC

REGISTRO DE DEUDA CONSOLIDADA: SISTEMA DE ADMINISTRACIÓN DEL CONSENTIMIENTO

SISTEMA DE ADMINISTRACIÓN DE CONSENTIMIENTOS REDEC

Plataforma para la obtención, registro, reporte y rendición de cuentas del consentimiento otorgado por los deudores, cumpliendo la Ley N° 21.680 Registro de Deuda Consolidada – REDEC.

CUMPLIMIENTO NORMATIVO



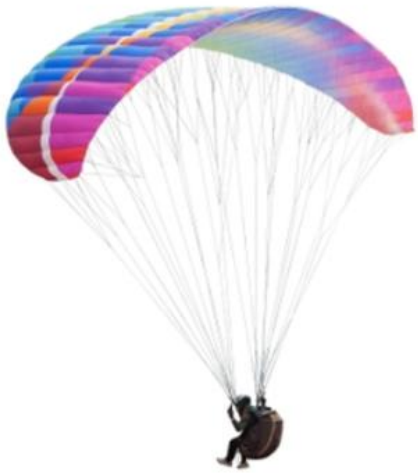
EXPERTCHOICE
first to reach the goal

Gestor de Consentimientos
REDEC

Descripción general

El software permite registrar, almacenar, administrar y auditar los consentimientos otorgados por titulares (personas naturales o empresas) a entidades (bancos u otras instituciones).

EL SISTEMA PROVEE:



- Registro del consentimiento
- Gestión de estados (otorgado, revocado, expirado)
- Evidencia digital
- Notificación al titular
- Trazabilidad Completa
- Acceso seguro y auditable

1.- ARQUITECTURA DEL SOFTWARE

El sistema consta de:

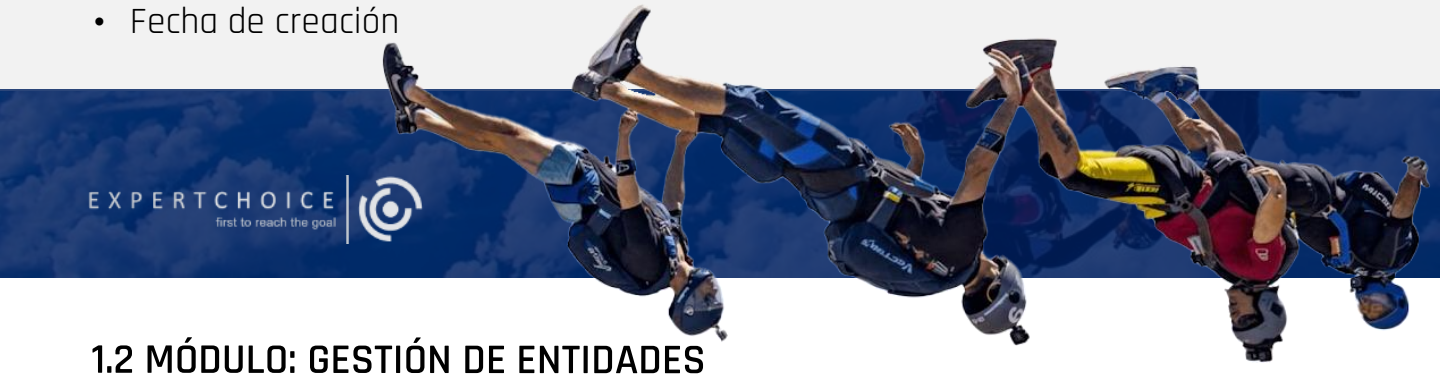
- Front ReactJS almacenado en AWS S3 y expuesto a través del CDN AWS CloudFront.
- Microservicios back Spring Boot montado en varias instancias AWS EC2 y balanceado.
- Base de datos RDS AWS.
- Identidad federada AWS Cognito.
- Concentrador de logs AWS CloudWatch.

1.1 MÓDULO: GESTIÓN DE TITULARES:

Descripción de Flujo de Uso.
El titular se registra a través del sistema POS de la institución Financiera, rellenando datos tales como rut, nombre, apellidos, correo, teléfono, entro otros. Para el caso de correo y teléfono, la institución financiera en POS habrá realizado una verificación con código para confirmar acceso del cliente a estos.
Para el cliente de la institución Financiera, será transparente el uso del Sistema de Administración de Consentimientos.

Campos clave
- RUT y DV
- Nombre
- Tipo de titular (persona / empresa)
- Email
- Teléfono
- Fecha de creación

Usos
- Crear titular.
- Consultar historial de consentimientos.
- Acceso portal del titular.



1.2 MÓDULO: GESTIÓN DE ENTIDADES

Descripción
Administra las entidades que solicitan consentimiento (bancos, financieras, etc.).

Campos clave
- RUT entidad
- Razón social

Usos
- Asociar entidad a consentimientos.
- Auditoría de accesos.

1.3 MÓDULO: GESTIÓN DE CONSENTIMIENTOS

Descripción

En pantalla de inicio, existe una sección con las últimas 3 acciones realizadas, junto con su estado (aprobado, rechazado, expirado). En caso de requerir el listado completo, se visualiza un botón Más Detalles para mostrar el histórico de consentimientos, y presionando botón Ojo, se muestra el detalle del consentimiento en particular, incluida la vigencia de este.
El consentimiento es digitalizado y encriptado según Anexo Técnico N°1 de la Norma de Carácter General N° 540 de la CMF. Se le envía notificación al titular del registro de este, y almacena en App copia de la notificación.

Campos clave

- Titular
- Entidad
- Estado actual (otorgado, revocado,
- expirado)
- Fechas legales
- Hash SHA-256
- Tipo de soporte (PDF / audio / JSON)

Usos

- Listado histórico de consentimientos.
- Aprobar o revocar un consentimiento.
- Validar estado de notificación hacia el titular.
- Acceso de detalle de consentimientos.

1.4 SEGURIDAD Y CONTROL DE ACCESO

Autenticación

- Identidad federada (Cognito / Azure AD / Google)
- JWT recibido en backend

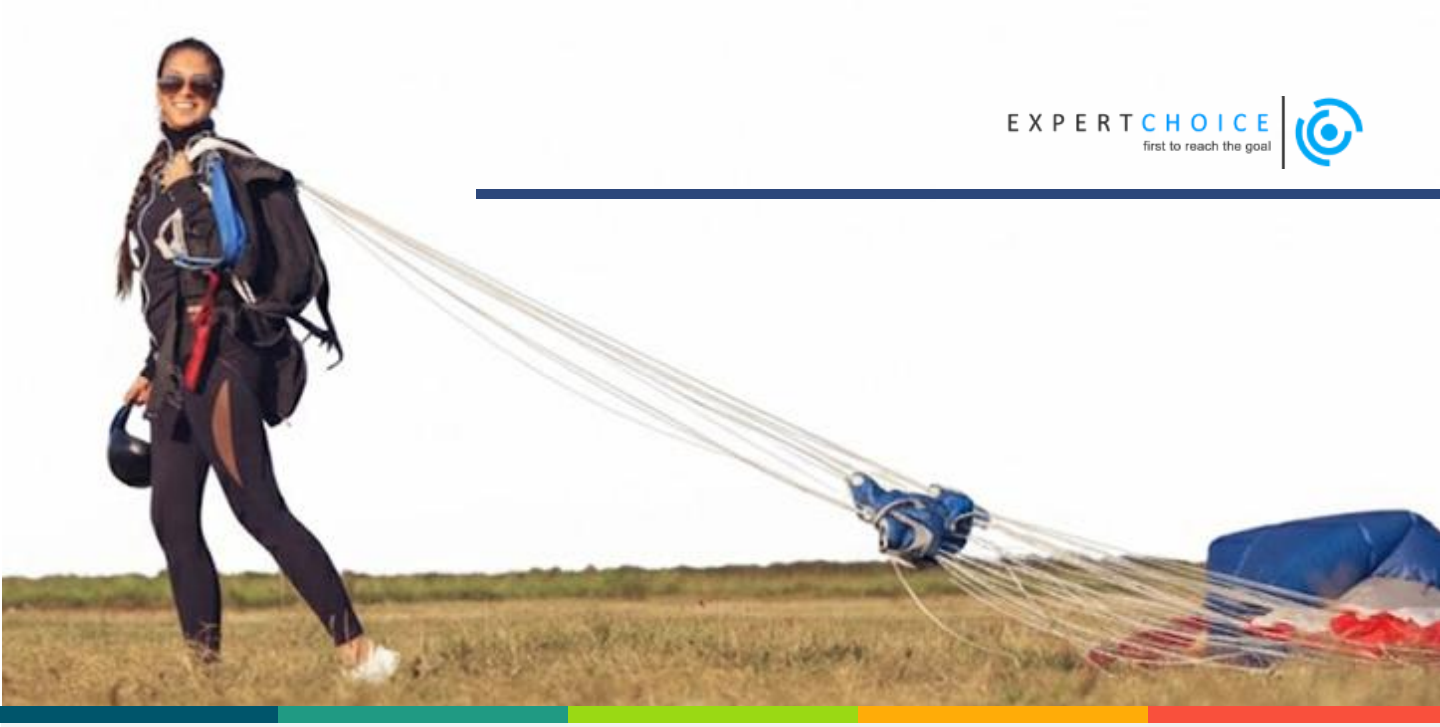
Autorización

- Roles internos del sistema
- Control a nivel de endpoint

Separación de roles

En el sistema existen N roles o perfiles, algunos de los cuales están descritos a continuación. Un usuario puede poseer más de uno.

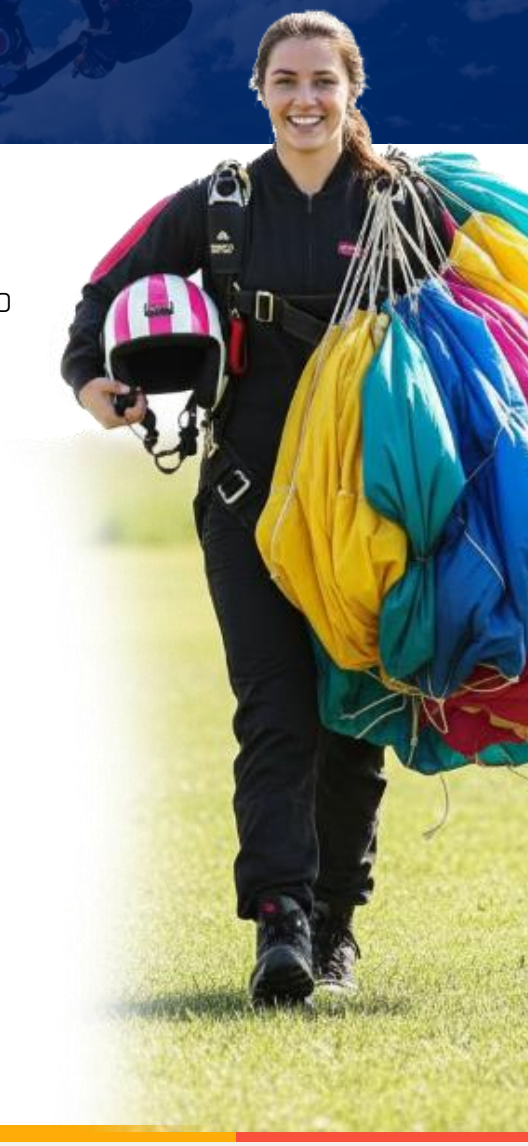
- **Administrador:** Perteneciente a entidad reportante, con acceso a todos los módulos de la App. Perfil otorgado por reportante.
- **Titular:** Perteneciente a la cuenta individual del titular, con acceso a gestionar sus consentimientos. Perfil asignado por defecto.



2.- AUTENTICACIÓN

El sistema utiliza un mecanismo de autenticación federada basado en los estándares OAuth 2.0 y JSON Web Tokens (JWT), permitiendo la integración con distintos proveedores de identidad reconocidos, tales como:

- AWS Cognito
- Azure Active Directory (Azure AD)
- Azure Active Directory B2C (Azure B2C)
- Google Identity



Este enfoque permite que la autenticación sea delegada a los sistemas de identidad propios del cliente o a proveedores externos de confianza, evitando la gestión directa de credenciales por parte de Expertchoice.

Una vez completado el proceso de autenticación, el proveedor de identidad emite un JWT firmado, el cual es recibido por la plataforma.

Expertchoice no almacena ni gestiona credenciales, limitándose a validar en el backend:

- La integridad criptográfica del token.
- Su vigencia temporal.
- El emisor y audiencia configurados.

Este modelo garantiza una autenticación segura, interoperable y alineada con buenas prácticas de seguridad y cumplimiento normativo.

3.- SEGURIDAD DE DATOS EN TRANSITO

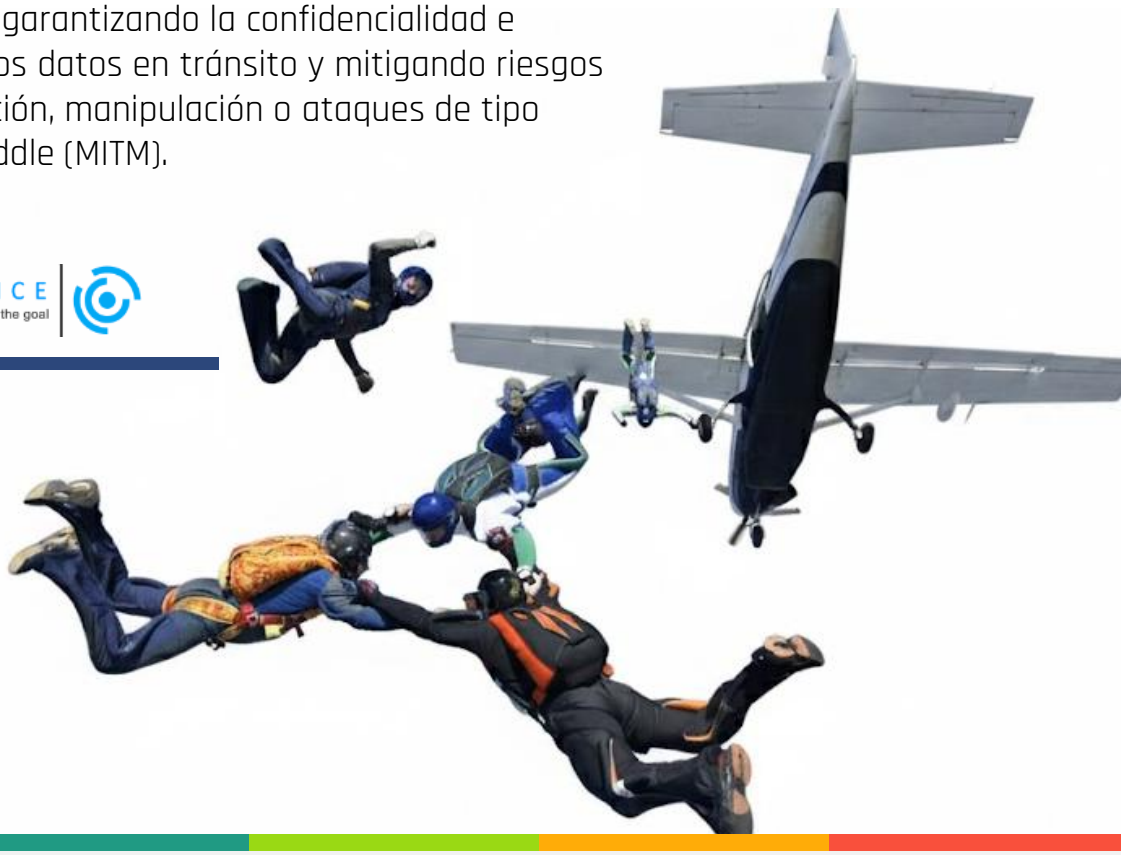
Tras la obtención del JWT, el usuario es redirigido al frontend de la aplicación. Desde este punto, todas las comunicaciones entre el frontend y los microservicios backend se realizan utilizando el token de acceso proporcionado por el proveedor de identidad.

La infraestructura de la plataforma se encuentra protegida mediante:

- AWS Application Load Balancer (ALB)
- AWS Certificate Manager (ACM)

Todo el tráfico entre el frontend y el backend se cifra utilizando TLS, garantizando la confidencialidad e integridad de los datos en tránsito y mitigando riesgos como intercepción, manipulación o ataques de tipo man-in-the-middle (MITM).

EXPERTCHOICE
first to reach the goal



4.- SEGURIDAD DE DATOS EN REPOSO

La información almacenada en la base de datos se encuentra protegida mediante cifrado en reposo, utilizando los mecanismos provistos por AWS Key Management Service (KMS).

Las claves de cifrado son administradas de forma segura por AWS, permitiendo:

- Protección de los datos almacenados en Amazon RDS (MariaDB)
- Rotación y gestión controlada de claves
- Cumplimiento con estándares de seguridad reconocidos

Este enfoque asegura que los datos permanezcan protegidos incluso ante accesos no autorizados a nivel de infraestructura.

5.- MÓDULO: ADMINISTRACIÓN DE ROLES

Módulo de la App que permita a roles Administrador actualizar perfiles de otros usuarios.

6.- NOTIFICACIONES DEL SISTEMA

Módulo de la App que permita a roles Administrador actualizar perfiles de otros usuarios.

6.1 A la App, le llegará una notificación cuando se solicite un consentimiento, la cual debe ser atendida por el titular. Para ello el titular ingresa al sistema, ve los detalles del consentimiento (Quien lo solicita, fecha, hora) y decide si aprobar o rechazar este. Para ambos casos anteriores, es requerido el ingreso del PIN previamente mencionado, regresando a la entidad solicitante una aprobación de esta.

6.2 Desde el sistema, es enviado a titulares su histórico de consentimientos cada 12 meses, a partir del registro en este. El contenido es la bitácora de consentimientos y el L&F es desarrollador por ExpertChoice, hasta que CMF defina.

6.3 Además del envío programado mencionado, se permite el envío de esta información, según lo desee el titular.

6.4 Enviar correo a email de reportantes, los cuales notifiquen cuando se obtiene el consentimiento del deudor.

7.- PARÁMETROS DEL SISTEMA

7.1 Tiempo de historia

Parámetro de que solicitudes, otorgamientos, revocaciones y acciones sobre consentimiento duran un máximo de 5 años en el sistema.

7.2 Correos reportante

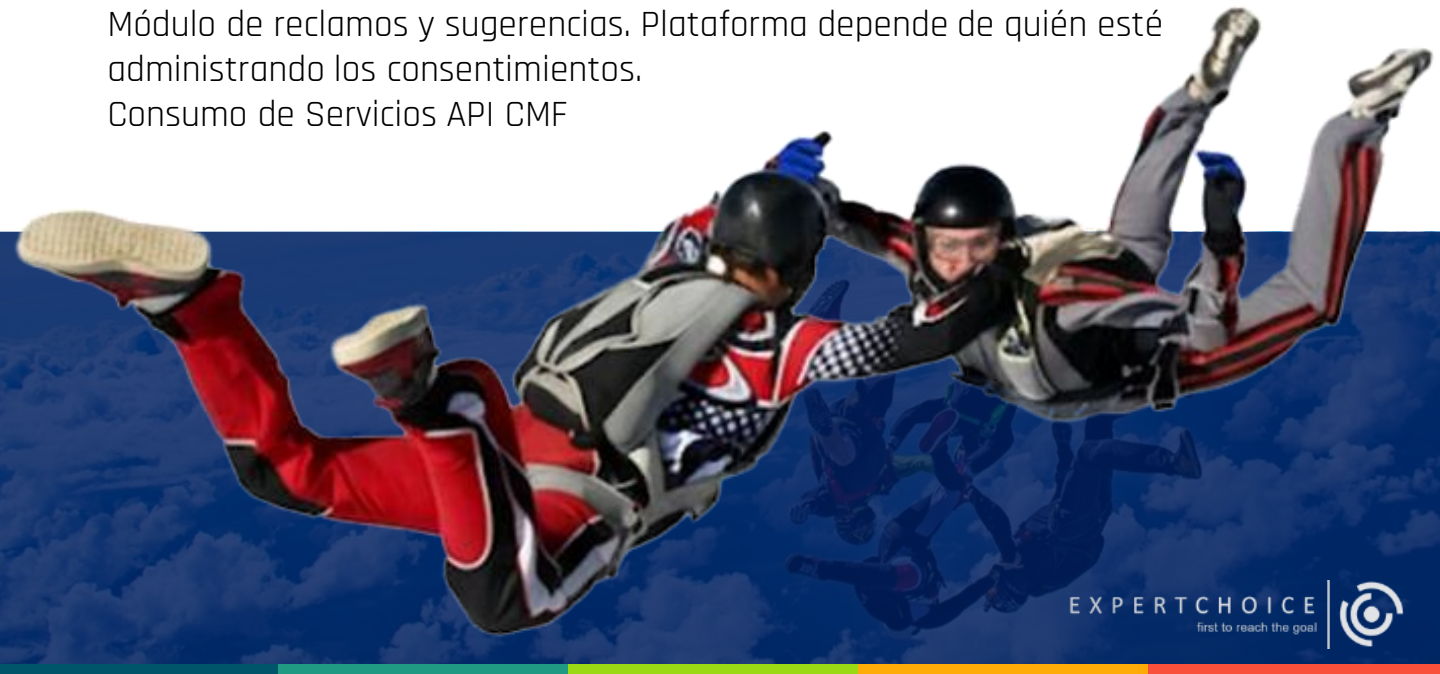
Parámetro para agregar correos de reportante, con el objetivo de ser notificados de novedades en el flujo.

7.3 Tiempo de validez de consentimiento

El consentimiento posee una vigencia de 15 días desde su aprobación, posterior a ese tiempo, este pasa a estado expirado.

8.- MÓDULO: PQR

Módulo de reclamos y sugerencias. Plataforma depende de quién esté administrando los consentimientos.
Consumo de Servicios API CMF



9.- CONSULTA DE INFORMACIÓN DE UN DEUDOR (RDC10)

- **Servicio:** consultaDeudaXConsentimiento
- **Propósito:** Obtener información del REDEC de un deudor que ha otorgado consentimiento a la institución reportante.

10.- Consulta de Requerimientos de Consentimiento

- **Servicio:** consultaReqConsentimiento
- **Propósito:** Canal para solicitudes de la Comisión de consentimientos digitalizados..

11.- Envío de Evidencia de Consentimiento

- **Servicio:** envioEvidenciaConsentimiento
- **Propósito:** Canal para que el reportante o mandatario adjunte documento digital del consentimiento solicitado por la Comisión

Gestor de Consentimientos
REDEC

SEGUIMIENTO Y MONITOREO

La plataforma implementa mecanismos de monitoreo y trazabilidad mediante el uso de AWS CloudWatch, el cual permite:

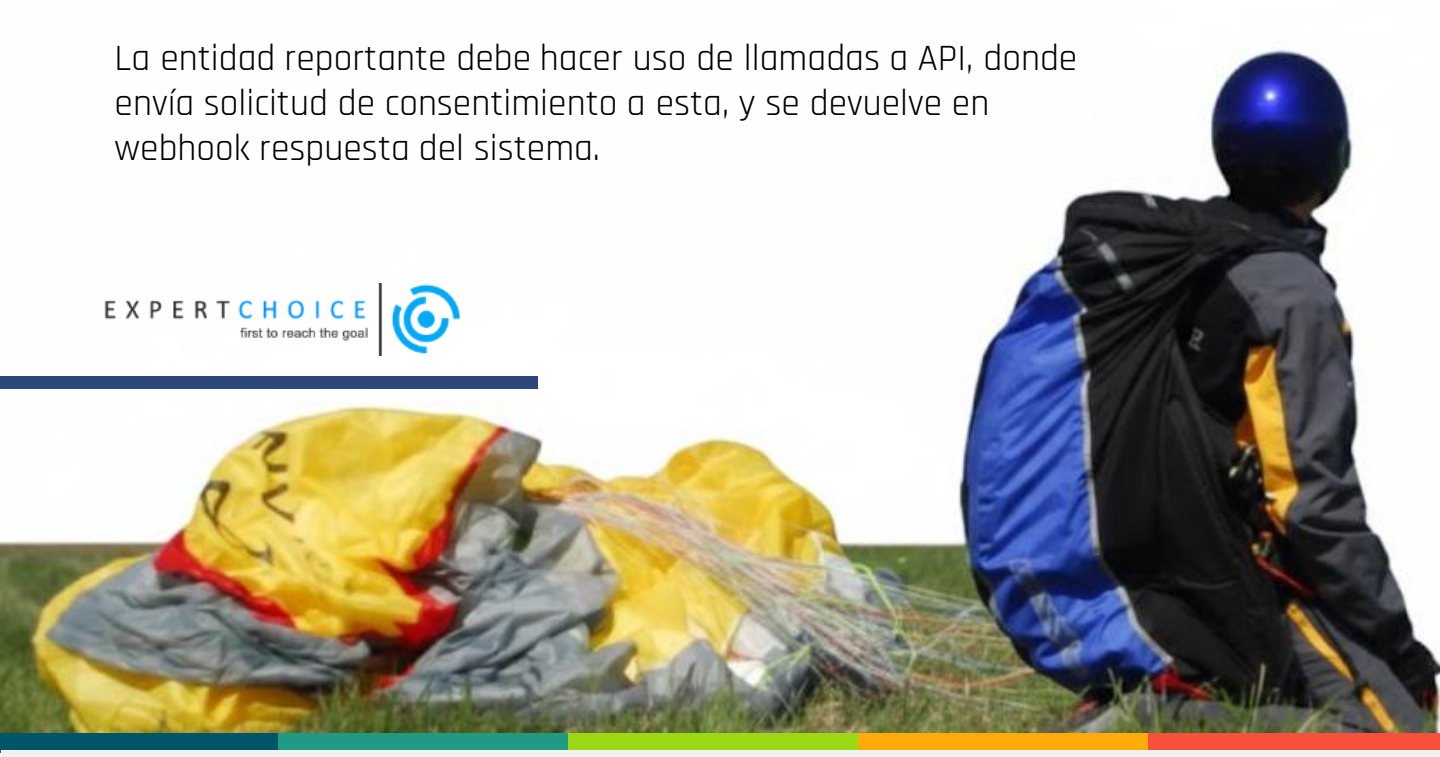
- Registro y almacenamiento de logs de aplicación
- Monitoreo de accesos y eventos relevantes
- Seguimiento de actividades realizadas por los usuarios
- Análisis de comportamiento y detección de incidentes

Los registros generados constituyen una fuente de evidencia para auditorías, análisis de incidentes y cumplimiento normativo, reforzando la transparencia y la capacidad de trazabilidad del sistema.

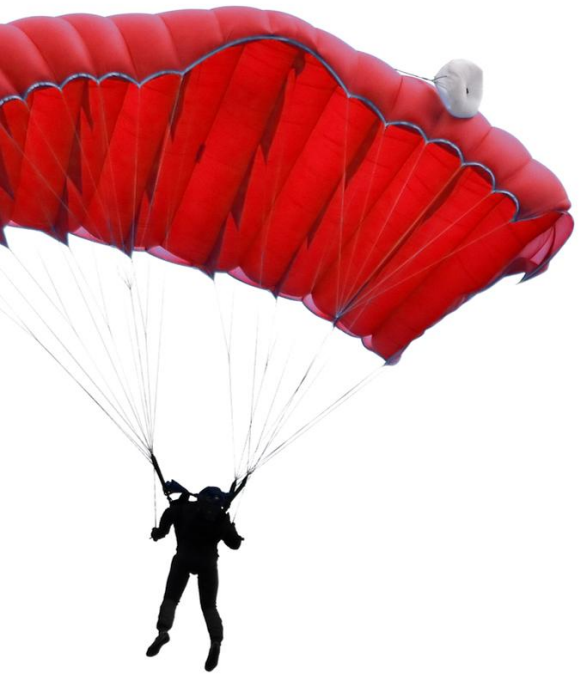
INTEGRACIÓN ENTIDAD REPORTANTE

La entidad reportante debe hacer uso de llamadas a API, donde envía solicitud de consentimiento a esta, y se devuelve en webhook respuesta del sistema.

EXPERTCHOICE
first to reach the goal



Gestor de Consentimientos
REDEC



Arquitectura AWS:

Rendimiento
Nuestros sistemas presentan **Up Time 99,8%** en versión Web, plan COB, ISO 27.001, replica geográfica.
Disponibilidad 24/7
Nivel transaccional de **26.000 por minuto.**
Arquitectura AWS Reciliente.
Tiempo respuesta promedio **menor a 1,8 segundos**
(Respuesta del aplicativo)

Disaster Recovery
RTO: 4 horas
RPO: Máx. 24 Horas.

Certificados ISO 27001